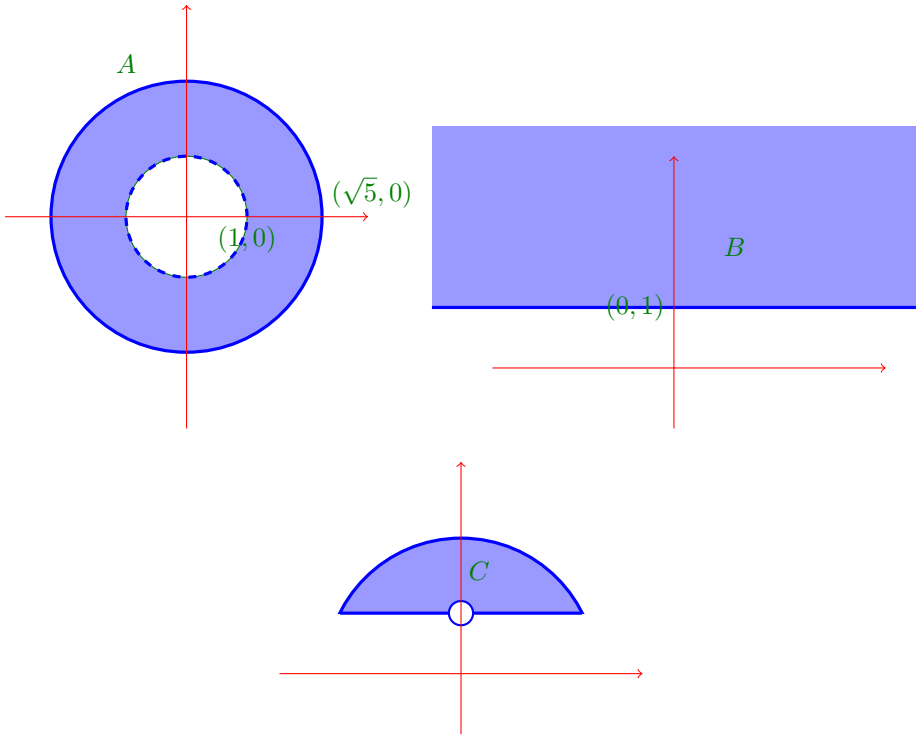
Formative solutions for TMA03 202xJ

TMA 03

Solution to Question 7 – 11 marks

(a) Sketches of the sets A, B and C are given in separate diagrams below: only a correct sketch of C is required for full marks. Notice the use of dashed and solid boundaries together with filled or open circles.



(b) To determine whether the limit of the sequence $\left((0,1+\frac{1}{n})\right)_{n=1}^{\infty}$ is in C, we need to identify what it is.

For large n, $\left(0,1+\frac{1}{n}\right)$ is going to be near to $(0,1)$, so we guess that the limit is likely to be $(0,0)$.

To show that the limit is $(0,0)$, we use Definition 3.4 of Chapter 13, which says that (for the Euclidean distance $d^{(2)}$), the limit of $\left((0,1+\frac{1}{n})\right)_{n=1}^{\infty}$ is $(0,1)$ if $\left(d^{(2)}\left(\left(0,1+\frac{1}{n}\right),(0,1)\right)\right)_{n=1}^{\infty}$ is a null sequence.

For $n \in \mathbb{N}$, we calculate

$$d^{(2)}\left(\left(0,1+\frac{1}{n}\right),(0,1)\right)=\sqrt{0^2+(1+\frac{1}{n}-1)^2}=\frac{1}{n}$$

and so $\left(d^{(2)}\left(\left(0,1+\frac{1}{n}\right),(0,1)\right)\right)_{n=1}^{\infty}$ is a null sequence. Hence the limit of the sequence is $(0,1)$.

Finally, we need to decide whether $(0,1) \in C$. C consists of the points that are both in A and B, so we need to check whether $(0,1) \in A$ and $(0,1) \in B$. Now $0^2+1^2=1$ and so $(0,1) \notin A$, meaning that $(0,1) \notin C$.

Solution to Question 8 – 14 marks

(a) (i) $x.f(x)=\sum_{i=0}^{n} a_i x^{i+1}$ (or $\sum_{i=1}^{n+1} a_{i-1}x^i$)

Copyright © 2020 The Open University

(ii) $(x+1).f(x) = a_0 + a_n x^{n+1} + \sum_{i=1}^{n}(a_i + a_{i-1})x^i$

$\left(= \sum_{i=0}^{n+1}(a_i + a_{i-1})x^i \quad \text{using the convention given in question} \right)$.

(iii)

$$\begin{aligned}(b_0 + b_1x + b_2x^2).f(x) = b_0a_0 &+ (b_1a_0 + b_0a_1)x \\ &+ (b_2a_0 + b_1a_1 + b_0a_2)x^2 + \cdots \\ &+ (b_1a_n + b_2a_{n-1})x^{n+1} + b_2a_nx^{n+2} \\ &= \sum_{k=0}^{n+2}\left(\sum_{i+j=k} b_ia_j\right)x^k.\end{aligned}$$

(b) Suppose that $f(x) = \sum_{i=0}^{n} a_ix^i$ and $g(x) = \sum_{j=0}^{m} b_jx^j \in \mathbb{Z}_7[x]$.
Then for $i = 0, \ldots, n$, $a_i \in \mathbb{Z}_7$ and for $j = 0, \ldots, m$, $b_j \in \mathbb{Z}_7$. Now,

$$\begin{aligned}f \cdot g &= \left(\sum_{i=0}^{n} a_ix^i\right)\left(\sum_{j=0}^{m} b_jx^j\right) \\ &= \sum_{i=0}^{n}\sum_{j=0}^{m} a_ib_jx^{i+j} \\ &= \sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_ib_j\right)x^k.\end{aligned}$$

Since $\mathbb{Z}_7$ is a ring, $\sum_{i+j=k} a_ib_j \in \mathbb{Z}_7$ and so $f \cdot g$ is a polynomial (of degree at most $m+n$) with coefficients in $\mathbb{Z}_7$. That is, $f \cdot g \in \mathbb{Z}_7[x]$, as required.

(c) (i) By definition a unit of $\mathbb{Z}_7[x]$ is a polynomial that has an inverse.
By Chapter 11, Lemma 2.9 p130, HB p50, the units of $\mathbb{Z}_7[x]$ are the constant polynomials: $1, 2, 3, 4, 5, 6$.

(ii) The definitions of associate and monic are given in
Chapter 11, Definition 2.11 p131, HB p50.
Since 4 is a unit of $\mathbb{Z}_7[x]$ (the inverse is 2), the unique monic polynomial that is an associate of 4 is 1.

(iii) The (multiplicative) inverse of 5 in $\mathbb{Z}_7$ is 3 and so the monic polynomial that is an associate of $5x^2 + 3$ is

$$3 \times (5x^2 + 3) = 15x^2 + 9 \equiv x^2 + 2.$$

Chapter 11, pp125–6, discussion after definition of polynomial ring
Chapter 11, p127, Exercise 2.1
Chapter 11, p130, Lemma 2.9
Chapter 11, p131, Exercise 2.4

Solution to Question 9 – 11 marks

(a) We check the axioms in Chapter 11, Definition 1.1 p112. Let $a, b, c \in \mathbb{Z}$.
First, we observe that $a \oplus b = b \oplus a$ and $a \odot b = b \odot a$ so **R5** and **R10** are satisfied. This saves some time with the other axioms.

R1: $a \oplus b = a + b + 1 \in \mathbb{Z}$ so $\oplus$ satisfies closure.

R2: $a \oplus (b \oplus c) = a + (b + c + 1) + 1 = (a + b + 1) + c + 1 = (a \oplus b) \oplus c$ so $\oplus$ is associative.

R3: $a \oplus (-1) = a + (-1) + 1 = a$ (and $(-1) \oplus a = a$ follows by commutativity R5) so the additive identity is (-1).

R4: $a \oplus (-2-a) = a + (-2-a) + 1 = -1$, so the additive inverse of a is $-2-a \in \mathbb{Z}$.

R6: $a \odot b = ab + a + b \in \mathbb{Z}$ so $\odot$ satisfies closure.

R7: $a \odot (b \odot c) = a(bc+b+c) + a + (bc+b+c) = abc+ab+ac+a+bc+b+c$ and
$(a \odot b) \odot c) = (ab+a+b)c + (ab+a+b) + c = abc+ac+bc+ab+a+b+c$, so $\odot$ is associative.

R8: $a \odot 0 = a \cdot 0 + a + 0 = a$ so 0 is the multiplicative identity.

R9: $a \odot (b \oplus c) = a(b+c+1) + a + (b+c+1) = ab + a + b + ac + a + c + 1 = (a \odot b) \oplus (a \odot c)$. The other case follows by commutativity of $\odot$, so we have distributivity.

(b) The 'zero' is -1, so if a is a zero divisor then there exists b such that $a \odot b = -1$. That is $ab + a + b = -1$, and so

$$a(b+1) = -(b+1).$$

From this, we conclude that $a = -1$ or $b = -1$ are the only possibilities, so there are no non-zero zero divisors. Therefore R is an integral domain.

(c) The multiplicative identity is 0, so if R is a field, then for any a there must exist b such that $a \odot b = 0$.

It suffices to take $a = 1$: from $0 = 1 \odot b = 2b + 1$ we find that

$$b = -\frac{1}{2}.$$

However, $b \notin \mathbb{Z}$, and so a does not have a multiplicative inverse. Therefore R is not a field.

Rings: Chapter 11, Exercises 1.1–1.2 p114

Zero divisors: Chapter 11, Exercises 1.6 p120

Integral domains: Chapter 12, Exercises 2.3, 2.4, 2.5(a) p191, 193

Fields: Chapter 11, Exercises 1.9, 1.10 p123–4

Solution to Question 10 – 14 marks

(a) The easiest way to do this is to observe that $N(a+b\sqrt{-n}) = a^2 + nb^2$ is multiplicative because it is equal to the complex modulus squared, which is itself multiplicative (see Chapter 12, discussion on p193.

Alternatively: Let $a + b\sqrt{-n}$ and $c + d\sqrt{-n} \in \mathbb{Z}[\sqrt{-n}]$.

Then

$$(a+b\sqrt{-n})(c+d\sqrt{-n}) = (ac - bdn) + (ad+bc)\sqrt{-n}$$

and so

$$\begin{aligned} N((a+b\sqrt{-n})(c+d\sqrt{-n})) &= (ac-bdn)^2 + n(ad+bc)^2 \\ &= b^2d^2n^2 + a^2d^2n + b^2c^2n + a^2c^2. \end{aligned}$$

However,

$$N(a+b\sqrt{-n}) = a^2 + nb^2 \text{ and } N(c+d\sqrt{-n}) = c^2 + nd^2.$$

Hence

$$\begin{aligned} N(a+b\sqrt{-n})N(c+d\sqrt{-n}) &= (a^2+nb^2)(c^2+nd^2) \\ &= b^2d^2n^2 + a^2d^2n + b^2c^2n + a^2c^2 \\ &= N((a+b\sqrt{-n})(c+d\sqrt{-n})), \text{ as required.} \end{aligned}$$

(b) We follow the method outlined in Exercise 2.6(a) of Chapter 12, page 194.

If u is a unit of $\mathbb{Z}[\sqrt{-n}]$, then there is $u^{-1} \in \mathbb{Z}[\sqrt{-n}]$ for which $uu^{-1} = 1$. But then $N(u) \times N(u^{-1}) = N(uu^{-1}) = N(1) = 1$ and so $N(u)$ divides 1, which implies that $N(u) = 1$, since $N(u) \geq 1$ for $u \in \mathbb{Z}[\sqrt{-n}] - \{0\}$.

Hence, if $u = a + b\sqrt{-n}$, then $N(u) = a^2 + nb^2 = 1$, meaning that $b = 0$ and $a = \pm 1$. Hence the only possible units in $\mathbb{Z}[\sqrt{-n}]$ are 1 and -1.

Finally, both $1 \cdot 1 = 1$ and $(-1) \cdot (-1) = 1$, and so 1 and -1 are both units in $\mathbb{Z}[\sqrt{-n}]$.

(c) See Exercise 2.5 of Chapter 12, page 193.

Since clearly $0 \neq 2$, to show that 2 is irreducible in $\mathbb{Z}[\sqrt{-n}]$ we must show that if we can write $2 = xy$, then one of x or y is a unit in $\mathbb{Z}[\sqrt{-n}]$.

So suppose that $2 = xy$ for some x and y in $\mathbb{Z}[\sqrt{-n}]$, then, since N is a multiplicative norm,

$$N(x)N(y) = N(xy) = N(2) = 4,$$

meaning that both x and y have norms that divide 4.

Hence both $N(x), N(y) \in \{1, 2, 4\}$.

If $N(x) = 4$, then $N(y) = 1$ and so, by the result in part (b), y is a unit.
If $N(x) = 1$, then by the result in part (b), x is a unit.

The only remaining possibility is that $N(x) = 2$ but if $N(a + b\sqrt{-n}) = a^2 + nb^2 = 2$, then since $n > 2$, we must have $b = 0$ and hence $a^2 = 2$. However, there are no integer solutions to this, so there are no elements with norm 2 in $\mathbb{Z}[\sqrt{-n}]$.

Thus, if $2 = x \cdot y$, then one of x and y is a unit. Hence 2 is irreducible.

(d) We have $N(\sqrt{-n}) = n$. Since $N(2) = 4$ does not divide n and N is multiplicative, we conclude that 2 cannot divide $\sqrt{-n}$.

(e) A non-zero non-unit element p of a ring R is prime if whenever $p|ab$ for $a, b \in \mathbb{R}$, then p either divides a or b. Chapter 12, Definition 2.6 p188, HB p54.

Since n is even, we can write $n = 2k$ for some (odd) integer k.

Thus 2 divides n. However, we can also write $n = -(\sqrt{-n}) \cdot (\sqrt{-n})$, but 2 divides neither of these factors.

Thus 2 is not prime, and hence by
Chapter 12, Corollary 4.3 (or Theorem 4.2) p206–7 $\mathbb{Z}[\sqrt{-n}]$ cannot be a UFD.

Chapter 12, Page 193, Exercise 2.5

Chapter 12, Page 194, Exercise 2.6(a)